OUCH! Maj 2020

SANS SECURITY AWARENESS

OUCH!

Biuletyn Bezpieczeństwa Komputerowego

Moc aktualizacji

Wstęp

Być może nie zdajesz sobie z tego sprawy, ale atakujący nieustannie szukają nowych podatności, czy słabości i je znajdują w oprogramowaniu, z którego korzystamy na co dzień. Takie oprogramowanie może być uruchamiane na Twoim laptopie, smartfonie, a nawet w niani elektronicznej i innych urządzeniach w Twoim domu. Atakujący wykorzystują znalezione słabości w oprogramowaniu, które umożliwiają im zdalne przełamanie zabezpieczeń w urządzeniach na całym świecie. Jednocześnie dostawcy oprogramowania i urządzeń stale opracowują poprawki podatności i wypuszczają je jako aktualizacje oprogramowania. Jednym z najlepszych sposobów, w jaki możesz się chronić, jest zapewnienie, że urządzania, z których korzystasz, mają najnowsze aktualizacje, co znacznie utrudnia włamanie się do nich.

Jak działa aktualizacja

Po wykryciu podatności, dostawca oprogramowania opracowuje i wydaje aktualizację (znaną również jako poprawka). Większość programów i urządzeń ma obecnie mechanizm łączenia się przez Internet z serwerem dostawcy w celu uzyskania aktualizacji oprogramowania. Taka aktualizacja, jest niczym więcej niż małym programem, który zazwyczaj instaluje się i usuwa lukę. Przykładami oprogramowania, które musisz aktualizować, są systemy operacyjne, na których działa Twój laptop (np. Microsoft Windows lub MacOS) lub smartfon (np. Android lub iOS). Często zapomina się, że powinno się aktualizować programy takie jak przeglądarka internetowa, edytor tekstu, oprogramowanie do przesyłania wiadomości lub aplikacje mobilne na telefonie (zwłaszcza aplikacje społecznościowe).

Dlatego za każdym razem, gdy kupujesz nowy program komputerowy lub nową aplikację mobilną, najpierw sprawdź, czy producent systematycznie je aktualizuje. Im dłużej oprogramowanie działa bez żadnych aktualizacji, tym bardziej prawdopodobne jest, że ma luki w zabezpieczeniach, które cyberprzestępcy mogą wykorzystać. Właśnie dlatego wielu dostawców, takich jak Microsoft, automatycznie wydaje nowe poprawki przynajmniej raz na miesiąc.

Jeśli nie używasz już określonego programu komputerowego, oprogramowania lub aplikacji mobilnej, usuń je z systemu. Im mniej oprogramowania musisz zaktualizować, tym bardziej jesteś bezpieczny.

Aktualizacja

Istnieją dwa ogólne sposoby na zaktualizowanie systemu:

- **Automatyczne:** Ilekroć urządzenie, system operacyjny, program lub aplikacja mobilna wykryje, że dostawca wydał nową aktualizację, automatycznie pobiera i instaluje aktualizację. Zaletą automatycznych aktualizacji jest to, że nie musisz nic robić. To oprogramowanie zapewnia, że używane technologie są aktualne. Wadą automatycznych aktualizacji jest to, że zaktualizowany program może powodować utratę funkcjonalności lub utratę danych. Co prawda, jest to rzadkie w przypadku osobistych urządzeń, ale może się zdarzyć w bardziej złożonych środowiskach, takich jak duże korporacje.

- **Manualne:** Kiedy pojawia się nowa aktualizacja urządzenia, systemu operacyjnego, programu lub aplikacji mobilnej, należy ją ręcznie pobrać i zainstalować. Daje to większą kontrolę nad tym, jakie aktualizacje są instalowane i kiedy to następuje. Większe organizacje (takie jak szpitale lub zakłady użyteczności publicznej) zazwyczaj korzystają z aktualizacji ręcznej, ponieważ umożliwia im to najpierw przetestowanie zmian, aby wykryć i rozwiązać wszelkie problemy. Wadą tego typu aktualizacji jest ich długi czas wykonywania i możliwość zaniedbania ich regularnego wykonywania.

Wnioski

Automatyczną aktualizację na wszystkich urządzeniach zalecamy wszystkim osobom prywatnym, rodzinom i małym biznesom. Dzięki temu wszystkie używane urządzenia, od smartfonów i laptopów po monitory i zamki do drzwi, są wyposażone w najnowsze oprogramowanie. Urządzenia i programy na bieżąco aktualizowane znacznie utrudniają atakującym złamanie zabezpieczeń. Włączenie automatycznych aktualizacji jest jednym z najprostszych i najskuteczniejszych sposobów aby się ochronić i móc w bezpieczny sposób korzystać z dzisiejszych.

Redaktor gościnny

Don C Weber jest liderem w dziedzinie bezpieczeństwa informacji z dużym doświadczeniem w zakresie DFIR, testów penetracyjnych i zarządzania od 2002 roku. Don uczestniczył w Komitecie Doradczym SANS, Ethics Committee, Gold Program, a obecnie jest instruktorem kursu ICS410. Szukaj Don jako @cutaway lub https://www.cutawaysecurity.com.

Źródła

Czy robisz kopie zapasowe: https://www.sans.org/security-awareness-training/resources/got-backups
Cztery proste kroki aby być bezpiecznym:
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz